Avoiding False Social Conformity in Majority-Malicious Connected Vehicle Networks Employing Consensus-Based Reputation Estimates

Gianna Voce
Department of Computer Science
Syracuse University
Syracuse, New York, USA
gtvoce@syr.edu

Henry Griffith
Department of Engineering
San Antonio College
San Antonio, Texas
hgriffith5@alamo.edu

Heena Rathore
Department of Computer Science
Texas State University
San Marcos, Texas
heena.rathore@txstate.edu

2024 IEEE International Conference on Consumer Electronics (ICCE) | 979-8-3503-2413-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICCE59016.2024.10444162

***Abstract*—Connected Vehicles (CVs) utilize real-time data exchange between vehicles and infrastructure to empower cooperative decision-making. This reliance on exchanged data introduces vulnerabilities related to the integrity of the shared data, which may be compromised by either malicious attacks or sensor failures. While consensus-based trust estimation algorithms offer a scalable solution for supporting data integrity, their reliability becomes limited for scenarios in which the majority of vehicle nodes are corrupted, a situation that mimics social conformity norms in humans. The research described herein demonstrates an approach for accurately estimating vehicle trustworthiness under majority-malicious network conditions. The Degroot model for distributed consensus formation is modified for vehicle trust estimation, which serves as input to a state-of-the-art cumulative reputation estimator. By drawing parallels between the behavioral tendencies observed in human social groups and the interactions among CVs, we aim to provide algorithmic enhancements that can mitigate the negative security vulnerabilities of conformity.**

***Index Terms*—connected vehicles, reputation, consensus, social psychology**

I. Introduction

Connected vehicles (CVs) are equipped with advanced sensing, communication, and computational capabilities that enable real-time data sharing with nearby vehicles and infrastructure [1]. Information is exchanged between vehicles in the network using a standardized protocol known as a basic safety message (BSM). This communication fosters cooperative decision-making [2], allowing vehicles to adapt to changing road conditions and traffic patterns more effectively. As these collaborative capabilities evolve, it becomes imperative to scrutinize vulnerabilities in CV networks resulting from data corruption that could compromise system performance.

There are two primary factors that can introduce data integrity vulnerabilities in CV networks. Firstly, malicious attacks represent intentional cyber aggressions intended to disrupt network operations through data falsification. Secondly, the sensors employed within CVs may fail as part of their normal life cycle, thereby also affecting data integrity. To mitigate the risks posed by these vulnerabilities, specialized algorithms have been devised to evaluate the integrity of data provided by each vehicle. This measure of cumulative data integrity is typically defined as the vehicle's reputation or trustworthiness [3]. CVs are especially well-suited for deploying consensus-based trust algorithms since the sensors of each node can be utilized to validate the BSMs reported by neighboring vehicles [4].

Consensus-based trust estimation involves the aggregation of individual trust estimates formulated on a per-vehicle basis across the entire network. This aggregation can be formulated using a variety of mathematical models, including Bayesian networks [5], distributed ledger techniques [12], and graph-based algorithms [6]. While these algorithms perform well when the majority of vehicles in a system are benevolent, performance is rarely ensured in majority-malicious conditions. These dynamics mimic the well-established concept of social conformity in humans.

Social conformity refers to individuals' tendencies to align their opinions, beliefs, and actions with the prevailing consensus of the group, even when they hold differing private convictions. For instance, the Asch conformity experiment, one of the most iconic studies in social psychology, vividly demonstrated the influence of group dynamics on individual behavior [7]. Participants, when faced with unanimous incorrect responses from a group of confederates, often conformed to the group's erroneous judgment, despite the evidence of their own senses. During the preceding decades, social conformity models have undergone extensive examination and application across diverse domains, aiming to amplify system efficiency by replicating human behavior [8]. The strengths of these models reside in their ability to gauge the gradual convergence of agents' viewpoints over time. In this study, we adopt the DeGroot opinion dynamics model of social conformity as a means to attain consensus among the vehicles within the system.

II. Related Work

A. Models for Trust and Reputation in CV

There are approaches aimed at enhancing trust, security, and reliability within networks of CV. Bayesian networks offer a probabilistic framework for capturing interactions among

vehicles, accommodating uncertain or incomplete data. In the work referenced by [5], the authors introduced a trust management model founded on Gaussian distributions, employing a Bayesian network. They amalgamated direct and indirect trust values to yield a final trust value, later fortified with input from third-party recommendations. For assessing the model's efficacy, a simulation of a disruptive on-off attack was executed using Matlab, with trust value and detection time as evaluation criteria. Outcomes indicated that the model exhibited quicker detection times and heightened accuracy in pinpointing on-off attacks.

Machine Learning (ML) excels at processing extensive data, recognizing non-linear associations, and autonomously extracting features. As detailed in [9], researchers introduced an artificial intelligence and statistical data classification framework for scrutinizing messages within CV. The model underwent training on the US Department of Transportation Safety Pilot Deployment Model, integrating a ML algorithm and a local trust manager. Empirical results manifested that the trained model proficiently anticipated false alerts, attaining a 98% precision rate, alongside a 0.55% standard deviation while facing 25% adversarial data.

Social network analysis, rooted in graph theory, is employed for detecting potential security vulnerabilities. Elucidated in [10], the authors used social network-driven bootstrapping methods for trust management within CV networks. This model accommodates initial trust values, node similarity, and a comprehensive trust and reputation management system, which accounts for historical behavior, facilitating enduring trust establishment. Simulations, executed through Colt libraries in Java, displayed the model's resilience against up to 60% of malicious nodes, achieving a worst-case precision of 74%.

Game-theoretic strategies emulate vehicle interactions as demonstrated in [6]. This research explores the feasibility of evaluating reputation management schemes for CV within dynamically evolving attack scenarios, through the lens of evolutionary game theory. The study simulates a CV network, introducing malevolent actors with randomly initiated attack strategies, and subsequently compares trust factor outcomes attained via evolutionary decision-making vis-à-vis static decision-making.

Blockchain-based algorithms create decentralized repositories of trust and reputation scores. Outlined in [11], researchers propose a multi-tier authentication and trust-building framework harnessing blockchain technology to enhance the reliability and integrity of shared information within CV. Experiments emulated a platoon structure, unveiling the interplay between blockchain mining duration, block generation frequency, and the influence of vehicle velocity on block creation.

B. Models for Social Conformity

For the past several decades, social psychology has been riveted by the phenomenon of social conformity. The movement began gaining attention in the 1950s when Solomon E. Asch carried out his famous conformity studies [15]. These studies had participants answer a simple question, such as comparing the length of two lines. In his most famous experiment, participants are given a card with one line drawn on it, and then another card with three other lines on it. One of the lines is the same as that on the first card, and the other two are noticeably different. The participants must then choose which line on the second card matches the length on the first. However, only one of the participants is the subject of the study, and the rest are hired to give the incorrect answer. All the hired participants respond inaccurately and the subject's answer is then observed. The majority of the time, the participant will agree with his cohort and answer erroneously, even though the correct answer is clear.

Several other experiments have been carried out proving this phenomenon and the factors that can affect it. Studies are often performed on the effects of gender [16], self-confidence [17], size of the group [18], etc. Typically, women conform more than men, lower confidence leads to a greater chance of conformity, and the size of the majority affects the degree of conformity [19]. Neuroscience studies have gone so far as to state that social conformity may be linked to reinforcement learning [20]but that claim is still up for debate [21]. It is easy to see the theoretical connections between conforming socially to a group and "fitting in" being seen as a reward to the human brain.

Social conformity not only caught the attention of the field of psychology but also mathematicians. In this respect, opinion dynamics is used by mathematicians that measure how people's opinions spread throughout a social network, and how different factors affect this spread, and how outlying opinions can persist throughout a disagreeing network. They have also been used for CVs such as in [22] which implemented the LuGre model to test the reliability of vehicle velocity reports in systems. One popular opinion dynamics model is the DeGroot model which offers a simple, yet effective way to model social opinions in a system. Its specific attributes will be elaborated on later in this paper.

III. Proposed Work

Several studies have explored the idea that CV behave as part of a social network, or have a "social brain." [25]. Frith and Frith [23] outline the steps taken in a "social brain" during a social interaction and many of the steps are comparable to parts of the reputation score calculation in CV. Exploring the concept of social-AI, particularly within the context of social CVs, reveals the intriguing possibility of applying theories from social psychology to these systems. Social conformity, a phenomenon of shared behavior, requires specific conditions to occur. These conditions encompass having agents in close proximity within a social network, all posed with the same question for which there are limited answers. These agents should possess a level of trust for their peers' opinions. They are then required to respond and share their answers with the network. Moreover, there needs to be some form of incentive for giving the "right" answer or consequences for the "wrong"

one. Considered as part of a social network, these vehicles are positioned within proximity. Each vehicle gives peer reports of other vehicles' kinematic data and, based on this, a reputation score is calculated. Depending on the system, the reputation of vehicles can rise or fall, constituting the reward or punishment element.

Social conformity materializes when there's a distinction between majority and minority opinions. In the context of CV networks, this occurs when a cyberattack corrupts the majority of the system. The corrupted vehicles might falsely label the uncorrupted minority as compromised. Consequently, the system becomes incapable of distinguishing malicious from benign vehicles. Drawing inspiration from the concept of social conformity and the belief that CVs function within a social network, potentially displaying conformity-like behaviors, this study intends to adopt a variation of the DeGroot model for calculating reputation scores in CV networks. Through this model, the objective is to accurately identify corrupt and uncorrupt vehicles even under conditions where the majority of vehicles are compromised.

A. The DeGroot Model

Taking a social network consisting of a number of agents *n*, each assigned an identifier, the DeGroot model will measure the spread of opinions across the network. Each agent communicates with their neighbors. Initially, every agent holds a binary opinion that denotes a specific claim. These opinions are organized in a vertical array, $x(0)$, where the position in the array corresponds to the agent's index within the system. In future iterations, $x(t)$ is the opinion matrix. A is a stochastic matrix whose rows indicate the vehicle's trust in other vehicles' opinions and will be referred to as the trust matrix. Specifically, $A_{i,j}$ denotes how much agent *i* trusts agent *j*'s opinion within the opinion matrix [24]. These opinions evolve over time, so an opinion matrix at any time *t* can be seen as:

$$x_{i,t} = A * x_{i,t-1} \tag{1}$$

As t increases, the group will reach an opinion consensus and all values in $x_{i,t}$ will be equal. The group consensus is measured as:

$$\lim_{t\to\infty} x_i = A^t(x(0)) \tag{2}$$

Where x_i is the group consensus opinion for agent *i*.

B. Reputation Update

Our approach incorporates a model introduced by Suo [13], inspired by Zacharia's [14] study on reputation systems, to update trust values. In the centralized scenario, a vehicle's calculated trust value is transmitted to the Trust Authority (TA) or Public Key Infrastructure (PKI) following a meticulous plausibility assessment. Subsequently, the TA employs a customized mechanism to update the trust value, factoring in various parameters like the learning factor θ and the impact of previous trust ratings (See Eq. 4). The maximum trust value D is adapted to reflect the TA's unwavering trust in its self-assessment, while the prior normalized trust value (E) also holds significant importance. Moreover, a damping function ϕ is introduced to regulate the influence of the previous trust value on the updated one.

$$R_{i,t}^{TA} = R_{i,t-1}^{TA} + \frac{\phi R_{i,t-1}^{TA} D(T_{i,t}^{TA} - E_{i,t-1}^{TA})}{\theta} \tag{3}$$

Here, $\phi(R_{i,t-1}^{TA}) = 1 - \frac{1}{1+exp\frac{-(R_{i,t-1}^{TA}-D)}{\sigma}}$ and $E_{i,t-1}^{TA} = \frac{R_{i,t-1}^{TA}}{D}$.

On the contrary, the distributed approach empowers any vehicle verifier (represented by (j)) to contribute its trust evaluation to the TA. In our context, $'j'$ pertains to the vehicle that issues the peer report of the vehicle nearby. The TA's trust update mechanism not only incorporates the verifier's evaluation but also takes into account the verifier's own credibility, as demonstrated in the following equation:

$$R_{i,t}^{TA} = R_{i,t-1}^{TA} + \frac{\phi R_{i,t-1}^{TA} R_{j,t-1}^{TA} (T_{i,t}^{j} - E_{i,t-1}^{TA})}{\theta} \tag{4}$$

This embodies the notion that an individual's reputation influences the perceived trustworthiness of their recommendations. This calculation takes place when the adjacent neighbors *j* are comparing their estimated positions to the reported position of agent *i* as described below. This is then used to update the value inside the opinion matrix to calculate the reputation scores for agent *i* at that time stamp.

C. Modified Model

To adapt the DeGroot model for CV use case the following modifications were made.

- *Updating opinions based on internal validity*: The reported coordinates of vehicle *i* is compared to the estimated coordinates given by its peer neighbor *j* [4]. If the two values are within a set threshold, vehicle *j* updates its opinion of vehicle *i* using Eq. 4. This opinion is updated inside of agent *i*'s opinion matrix and the updated matrix is fed into Eq. 5 to generate the new opinions to be used in the next time iteration.
- *Introducing weight matrix*: In order to add a layer of validity dependent on past performance, a weight matrix is introduced. When a reported estimation aligns with the existing estimation, the significance of both vehicles is augmented to a weight of 2 within the matrix. Conversely, if the reported estimation diverges from the existing one, the weight remains at 1.
- *Removing agent self-confidence*: The DeGroot model often considers a measure of self-confidence that is stored along the diagonals of the trust matrix at position A_{ii}. In order to guard against over-self-confidence, the trust matrix is updated to have 0s along the diagonals. A similar approach is taken in the opinion matrix.

Thus with these adaptions, the equation is as follows.

$$x_{i,t} = W * A * x_{i,t-1} \tag{5}$$

where, $x_i(t)$ is the opinion matrix which, for CV represents the reputation of vehicle *i*. *W* denotes the weight matrix. The algorithm first checks if a vehicle is within the designated

adjacency range. Once vehicles are confirmed to be within this range, estimations and reputation calculations are performed. If vehicles are not within the range, a default level of trust is assumed. The algorithm calculates reputation scores for each vehicle individually. These individual scores are then averaged to compute a mean score. This mean score is used in the following time iteration. The incorporation of this mean score substantially improves both the speed of convergence and the accuracy of calculations, leading to an overall enhancement in the algorithm's performance.

IV. Results

A. Dataset

Department of Transportation dataset on Multi-Modal Intelligent Traffic Signal Systems (MMITS) [27] contains BSMs from thirteen vehicles' Global Positioning System (GPS) was used in order to test the model. For testing, only the first 30,000 rows of the dataset were used, which contained BSMs from seven vehicles over roughly twenty-one hours (74,455 seconds). This data was processed in a Python script that randomly corrupted a selected percentage of vehicles' data and then used the model to calculate reputation scores.

B. Attack Models

Our model was tested on four different types of attacks namely constant offset, ON-OFF, drift, and chronic.

1) Constant Offset Attack: A constant offset attack simulation was conducted by adding constant faulty sensor readings in the dataset using the longitude data of the vehicles:

$$s'(t) = s(t) + s(t) * r \tag{6}$$

Where $s(t)$ is the uncorrupted measurement and $s(t) * r$ represents the constant offset amount to be added to the original signal. Offsets of +.5 and +10 were added to the estimated x position of the vehicle. In a system that is 90% corrupt, five of the vehicles are corrupted and one is not. Figure 1 shows the reputation scores of the vehicles in the system with +10 offset. Corrupted Vehicles are shown in red, uncorrupted in green.

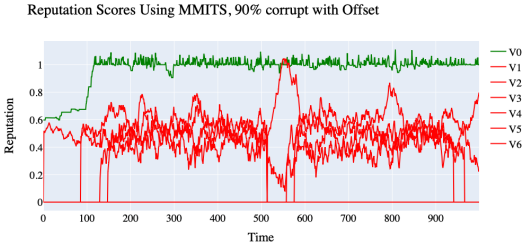

Fig. 1. Reputation scores vs time (sec) in system with 90% off-set corruption

2) ON-OFF Attack: White Gaussian noise attack was introduced using a method involving the creation of a windowing function to establish an alternating "ON-OFF" parameter.

$$s(t) = s(t) + \eta(t).w(t) \tag{7}$$

Here, $w(t)$ takes values of either 0 or 1, embodies the characteristics of the windowing function. It is defined by stochastic parameters that capture the temporal dynamics of the ON-OFF attack. Specifically, when w(t) is zero, the attack is inactive (OFF), while a value of one signifies its activation (ON).

Performance was tested with ON-OFF attacks that turned on or off every 10 iterations or every 100 iterations. Figure 2 shows a graph of reputation scores in a system that is 90% corrupt and with corruption that turns on every 100 iterations for 100 iterations and then turns off.

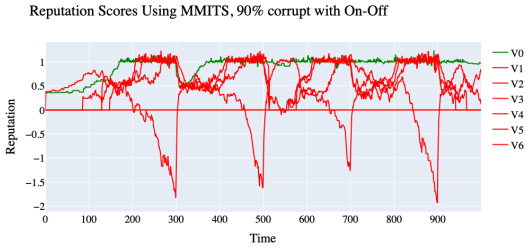

Fig. 2. Reputation scores vs time (sec) in system with 90% on-off corruption

3) Drift Attack: In this, we introduce a signal manipulation by inducing a gradual drift or shift in the signal's values. In our approach, a drift function is introduced to determine the rate and direction of the drift, resulting in the following expression:

$$s(t) = s(t) + d.t \tag{8}$$

Here, d represents the drift component and t represents time step, dictating the extent of the shift applied to the signal at each time point. Figure 3 shows reputation scores in a system that is 90% corrupt with drift corruption that accumulates at a rate of 5 times the time step. Drift of 10 times the time-step was also tested with similar results.

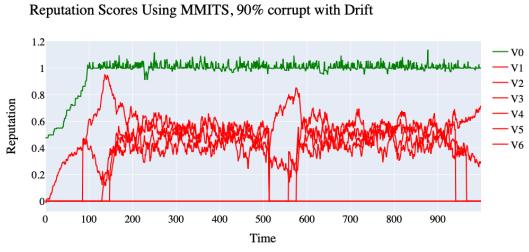

Fig. 3. Reputation scores vs time (sec) in system with 90% drift corruption

4) Chronic Attack: The chronic attack model introduces a unique form of distortion characterized by an initial increase in values similar to a drift, followed by a subsequent decrease.

$$s(t) = s(t) + t.g(t) \tag{9}$$

In this equation, $g(t)$ embodies the behavior of the chronic function, which defines how the chronic attack evolves over time. Chronic corruption was tested by adding 10 times the iteration number for half the simulation time, and then subtracting 10 times the iteration number. This is shown in Figure 4 with 90% corruption.

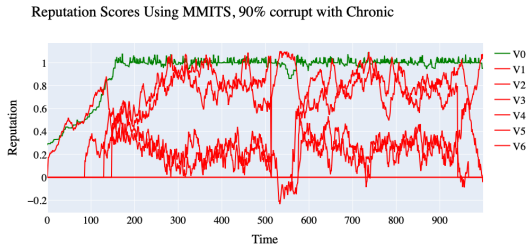

Fig. 4. Reputation scores vs time (sec) in system with 90% chronic corruption

Figure 5 shows the difference between using the reputation update discussed in III.C vs updated opinions in a binary fashion (0 or 1). The addition of reputation update significantly increases the reputation of uncorrupted vehicles and allows for easier distinction between corrupt and uncorrupt vehicles.

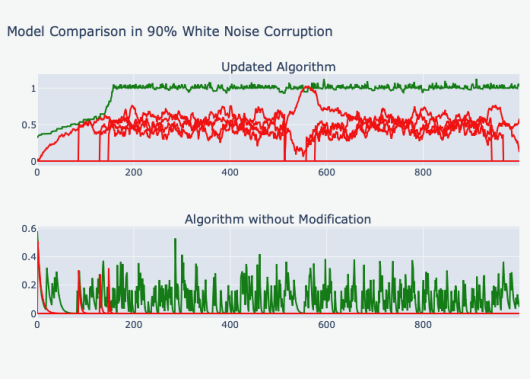

Fig. 5. Reputation scores vs time (sec) between the two models

Figure 6 shows the effect of varying the values for θ and σ, which are the learning and forgetting factors. The vehicle graphed was uncorrupted in a system that was 90% corrupted with white noise. Results for the rest of the study were generated using a θ value of 1.2 and a σ value of 0.2.

Similarly, a corrupt vehicle from each kind of corruption was graphed in three different levels of corruption (50%, 75%, and 90%). Figure 7 shows the reputation scores of a corrupted vehicle for each kind of fault: chronic, drift, white noise, on-off, and offset, in that order.

C. Comparison

We compared our model to two different algorithms, TangleCV [12] and a Bayesian-based algorithm [26]. Figure 8 shows the reputation under the Bayesian algorithm. As seen from the figure, the reputation of corrupted and uncorrupted vehicles cannot be distinguished. TangleCV was chosen as a comparison because of its nature as a social psychology-based

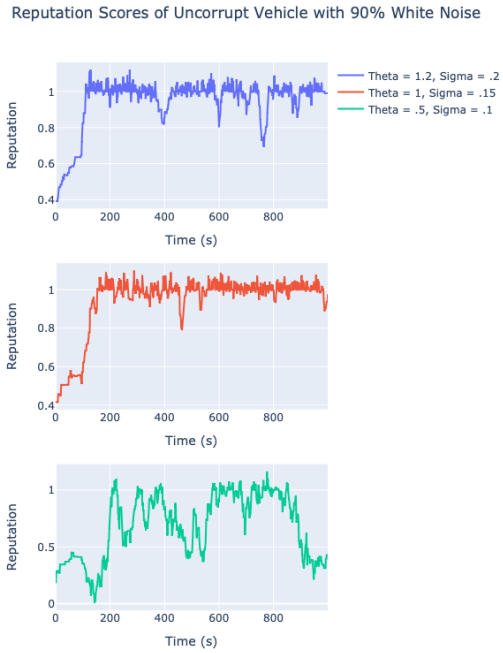

Fig. 6. Reputation scores vs time (sec) comparing various θ and σ values

algorithm and Bayesian was chosen because of its popularity among reputation score algorithms. We compared these algorithms in all four kinds of corruption with a corruption level of 90%. Across levels of corruption, the DeGroot model showed the most consistent high performance.

V. Conclusion

This paper proposed an opinion dynamics model for achieving consensus in CV networks to establish trust. The results were validated on MMITS dataset. The model yielded accurate results with a fast convergence rate in majority malicious conditions. It effectively identifies malicious and benevolent vehicles in the presence of majority-malicious scenarios, with F1-scores ranging from 0.92 to 1.0. It demonstrates consistent performance across different corruption levels, with the enhanced reputation scheme contributing to improved results.

Acknowledgment

This publication has been supported by NSF CISE Research Initiation Initiative (CRII) grant #2153510 and #2313351.

References

[1] D. Yang et al., "Intelligent and connected vehicles: Current status and future perspectives". *Science China Technological Sciences*, 61, pp.1446-1471, 2018.

[2] S.Y. Gelbal et al., "Cooperative collision avoidance in a connected vehicle environment". arXiv preprint arXiv:2306.01889, 2023.

[3] H. Rathore, and H. Griffith, "GNN-RL: Dynamic Reward Mechanism for Connected Vehicle Security using Graph Neural Networks and Reinforcement Learning". In 2023 IEEE International Conference on Smart Computing (SMARTCOMP), pp. 201-203, 2023.

Fig. 7. Reputation scores vs time (sec) comparison between 50%, 75%, and 90% in corruption

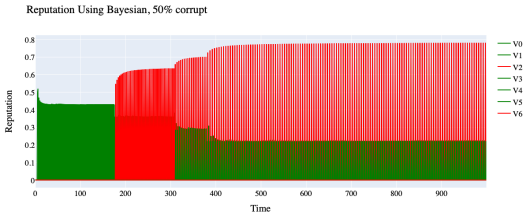

Fig. 8. Reputation score for under Bayesian Algorithm for 50% corruption

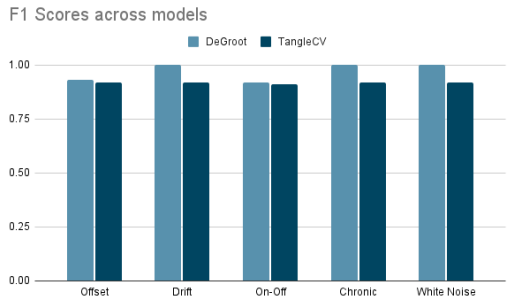

Fig. 9. F1 Score Comparison across models

[4] H. Griffith, M. Farooq and H. Rathore, "A Data Generation Workflow for Consensus-Based Connected Vehicle Security," 2023 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, pp. 1-2, 2023.

[5] W. Fang et al.,"BTDS: Bayesian-based trust decision scheme for intelligent connected vehicles in VANETs",*Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 12, p.e3879, 2020.

[6] Z. Tian et al., "Evaluating Reputation Management Schemes of Internet of Vehicles Based on Evolutionary Game Theory," in *IEEE Transactions on Vehicular Technology*, vol. 68, no. 6, pp. 5971-5980, 2019.

[7] K.S. Larsen. "The Asch conformity experiment: Replication and transhistorical comparison". *Journal of Social Behavior and Personality*, vol. 5, no. 4, p.163, 1990.

[8] Y. Peng, Y. Zhao, and J. Hu, "On the role of community structure in evolution of opinion formation: A new bounded confidence opinion dynamics". *Information Sciences*, 621, pp.672-690, 2023.

[9] E.O. Eze et al., "A Context-Based Decision-Making Trust Scheme for Malicious Detection in Connected and Autonomous Vehicles". in Proc. *IEEE2022 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*, pp. 31-36, 2022.

[10] D. Alishev et al., "Social-aware bootstrapping and trust establishing mechanism for vehicular social networks". In *2017 IEEE 85th Vehicular Technology Conference (VTC Spring*, pp. 1-5, 2017.

[11] F. Kandah, et al., "BLAST: Blockchain-based trust management in smart cities and connected vehicles setup". In *2019 IEEE High Performance Extreme Computing Conference (HPEC)*, pp. 1-7, IEEE, 2019.

[12] Rathore, H., Sai, S. and Gundewar, A., 2023. Social Psychology Inspired Distributed Ledger Technique for Anomaly Detection in Connected Vehicles. IEEE Transactions on Intelligent Transportation Systems.

[13] D. Suo, "Towards security by design of connected and automated vehicles: cyber and physical threats, mitigations, and architectures" (Doctoral dissertation, Massachusetts Institute of Technology), 2021.

[14] G. Zacharia and P. Maes. "Trust management through reputation mechanisms". *Applied Artificial Intelligence*, 14(9):881–907, 2000.

[15] Asch, S.E., 1955. Opinions and social pressure. Scientific American, 193(5), pp.31-35.

[16] K. Mori, and M. Arai, "No need to fake it: Reproduction of the Asch experiment without confederates". *International Journal of Psychology*, vol. 45, no. 5, pp.390-397, 2010.

[17] C. P. Cross et al., "Sex differences in confidence influence patterns of conformity". *British Journal of Psychology*, vol. 108, no. 4, pp.655-667, 2017.

[18] S. Sowden et al., "Quantifying compliance and acceptance through public and private social conformity". *Consciousness and cognition*, 65, pp.359-367, 2018.

[19] S.C. Goldberg, "Three situational determinants of conformity to social norms". *The Journal of Abnormal and Social Psychology*, vol. 49, no. 3, p.325, 1925.

[20] V. Klucharev et al., "Reinforcement learning signal predicts social conformity". *Neuron*, vol. 61, no. 1, pp.140-151, 2009.

[21] M. Levorsen et al., "Testing the reinforcement learning hypothesis of social conformity". *Human Brain Mapping*, vol. 42, no. 5, pp.1328-1342, 2021.

[22] E. Hashemi et al., "Opinion dynamics-based vehicle velocity estimation and diagnosis." *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 7, pp.2142-2148, 2017.

[23] U. Frith, and C. Frith, "The social brain: allowing humans to boldly go where no other species has been". *Philosophical Transactions of the Royal Society B: Biological Sciences*, vol. 365, no. 1537, pp.165-176, 2010.

[24] Lecture 5: The DeGroot Learning Model (PDF) "https://ocw.mit.edu/courses/14-15-networks-spring-2022/resources/mit14_15s22_lec5/" [Accessed on August 15, 2023]

[25] S. W. Loke, "Cooperative Automated Vehicles: A Review of Opportunities and Challenges in Socially Intelligent Vehicles Beyond Networking," in *IEEE Transactions on Intelligent Vehicles*, vol. 4, no. 4, pp. 509-518, 2019.

[26] Y. Begriche et al, "Bayesian-based model for a reputation system in vehicular networks," in Proc. *International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, pp. 1-6, 2015.

[27] Multi-Modal Intelligent Traffic Signal Systems GPS, https://datahub.transportation.gov/Automobiles/Multi-Modal-Intelligent-Traffic-Signal-Systems-GPS/2f79-bkh3/data [Accessed on August 15, 2023].